Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A monitoring device disposed for thwarting denial of service attacks on ~~the~~ a data center, the monitoring device comprising:

a plurality of probe devices that are disposed to collect statistical information on packets that are sent over links that couple ~~between~~ the network ~~and~~ to the data center;

a cluster head coupled to each of the plurality of probe devices, the cluster head receiving collected statistical information from the probe devices and determining from the collected information whether the data center is under a denial of service attack.

2. (Currently Amended) The device of claim 1 wherein the cluster head is coupled to the plurality of probe devices through a dedicated, private network, that is a different network from the network being monitored.

3. (Previously Presented) The device of claim 2 wherein the cluster head further comprises:

a communication process that sends statistics collected by the probe devices to a control center, and that receives queries or instructions from the control center.

4. (Original) The device of claim 3 wherein the monitoring device is a gateway device and further comprises:

a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack.

5. (Currently Amended) The device of claim 1 wherein the probes are physically deployed in line in the links that couple the network to the data center with each of the probes deployed to monitor one or more links.

6. (Previously Presented) The device of claim 1 wherein the probes execute a joining process that allows the probes to join ~~a cluster~~ the device.

7. (Previously Presented) The device of claim 1 wherein the cluster head comprises a process to aggregate statistics collected from the probes and to produce logs and apply detection heuristics to the statistics collected from the probes.

8. (Currently Amended) A method of thwarting denial of service attacks on a victim data center coupled to a network comprises:

monitoring network traffic through probes that are disposed to monitor packets over links that couple ~~between~~ the victim data center and the network; and

communicating data from the probes, over a dedicated network, to a cluster head device.

9. (Original) The method of claim 8 further comprising:

communicating data from the cluster head device to a control center over a hardened network.

10. (Original) The method of claim 8 further comprising:

analyzing network traffic statistics to identify malicious network traffic; and

filtering network traffic, which is identified as malicious network traffic, during analyzing of the network traffic.

11. (Previously Presented) The method of claim 8 further comprising

providing the cluster head device and the probe devices as a clustered gateway.

12. (Previously Presented) The method of claim 11 wherein when a new cluster probe seeks to join to the clustered gateway, the method further comprises:

dynamically discovering the new cluster probe that seeks to join the clustered gateway.

13. (Original) The method of claim 8 further comprising:

performing intelligent traffic analysis and filtering to identify the malicious traffic and to eliminate the malicious traffic.

14. (Original) The method of claim 13 wherein performing intelligent traffic analysis is controlled by the cluster head and filtering is performed by the probes.

15. (Previously Presented) A gateway for thwarting denial of service attacks on a victim data center comprises:

a cluster head; and

a plurality of probes disposed to monitor links that couple ~~between~~ a network and a victim data center, the probes collecting statistical data, for performance of intelligent traffic analysis and filtering by the probes, to identify malicious traffic for thwarting denial of service attacks.

16. (Original) The gateway of claim 15 wherein the gateway includes a process to insert filters to discard packets that are deemed to be part of an attack.

17. (Previously Presented) A monitoring device disposed for thwarting denial of service attacks on a data center, the monitoring device comprising:

a device that collects statistical information on packets that are sent between the network and the data center over a plurality of links and that produces statistical information from

network traffic over the plurality of links to determine from the statistical information whether the data center is under a denial of service attack.

18. (Original) The monitoring device of claim 17 wherein the monitoring device is coupled to a control center through a hardened network.

19. (Original) The monitoring device of claim 17 wherein the device further comprises:

a communication process that communicates statistics with a control center, and that receives queries or instructions from the control center.

20. (Original) The monitoring device of claim 17 wherein the monitoring device is a gateway device and further comprises:

a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack.

21. (Previously Presented) The monitoring device of claim 20 wherein the gateway comprises:

a process to aggregate statistics collected from the various links and to produce logs and detection heuristics concerning the statistics collected from the probes.

22. (Currently Amended) A method of thwarting denial of service attacks on a victim data center coupled to a network comprises:

monitoring network traffic over a plurality of links between the victim data center and the network; and

communicating data to a control center, with communicating occurring [[,]] over a ~~hardened~~ redundant network that is a different network from the network being monitored~~, to a control center~~.

23. (Original) The method of claim 22 wherein monitoring is performed by probe devices that sample network traffic at a constant rate.

24. (Previously Presented) The method of claim 23 further comprising:

delivering the sampled network traffic by the probes to a clustered head for traffic analysis.

25. (Previously Presented) The method of claim ~~23~~ 24 wherein the probes send the sampled network traffic to the cluster head at a substantially constant rate irrespective of traffic on the monitored network.

26. (Previously Presented) The device of claim 1 wherein the probes are coupled between the network and the data center to monitor traffic on links that couple the data center to the network.

27. (Previously Presented) The device of claim 1 wherein the probes are scaleable and can dynamically join or leave the cluster.

28. (Previously Presented) The device of claim 1 wherein the cluster head analyzes traffic on the links and treats the traffic on the monitored links as if the traffic originated on one virtual link.

29. (Previously Presented) The device of claim 1 wherein at least one of the probes examines packets sent across the link that the at least one probe monitors and randomly chooses selected numbers of packets per second to pass to the cluster head.

30. (Previously Presented) The method of claim 8 wherein monitoring comprises disposing the probes to monitor traffic on links that couple the data center to the network.

31. (Previously Presented) The device of claim 15 wherein the probes are coupled between the network and the data center to monitor traffic on links that couple the data center to the network.

32. (Previously Presented) The device of claim 18 wherein the probes are coupled between the network and the data center to monitor traffic on links that couple the data center to the network.